CALIFORNIA SECURITY INCIDENT REPORTING FORM

This submission is required by Calif. Civil Code s. 1798.29(e); Calif. Civ. Code s. 1798.82(f)

[11/20/2012]

Note: This form is only for use by businesses and state agencies, which are required to submit a sample notice if they experience of breach of personal information involving more than 500 California residents.

1.) Log into website: https://www.oag.ca.gov/ecrime/databreach/report-a-breach

Section I – Attach Security Breach Notification Sample

- Upload Customer letter (AD01) – (PDF document only)
- Organization Name:
  - American Express Travel Related Services Company, Inc and /or its Affiliates ("AXP")
  - 200 Vesey Street, 3 World Financial Center
  - New York, NY 10285
- Date(s) of Breach (if known)
  - 2012-08-03
- Enter Captcha - This question is for testing whether you are a human visitor and to prevent automated spam submissions.
- Date(s) Individual Notice Provided to Consumers
- Enter Consumer notification date: 11/9/2012
- Enter Corporate date (if applicable): 11/16/2012
- Was notification delayed because of a law enforcement investigation?
  - Select appropriate response (No)
- Type of Personal Information Involved in the Breach
  - Highlight line(s) item(s) as appropriate
- Brief Description of the Breach
  - Merchant name, address, case number: C2012095824
    - Paygate (multiple locations if applicable)
    - Location 1 Address: 11 Vans Rd Suite B3, Tokai Village Centre, Toakai, Cape Town, South Africa
- Case summary concise narrative: Evidence available indicates an attacker was able to use an insufficiently protected Merchant Management Interface file upload facility to upload malicious web scripts to the server for which legitimate customers use. The attacker has able to alter one of the primary cardholder data processing scripts to siphon off cardholder data as it is being entered into each client's website for processing.
- Report Type
  - Select appropriate response (Initial Breach Report)
- Breach Affecting
  - Select appropriate response (500 or More Individuals)
- Approximate Number of Individuals Affected by the Breach
  - Enter CA impacted Individuals: 1031

- Type of Entity
    - BSR – Businesses – Retail or Merchant
- Type of Breach
    - Select appropriate response (Unintended disclosure, Hacking or malware, Payment Card Fraud, Insider, Physical Loss, Portable device, Stationary device, Other) Hacking or Malware
        - If "Other" please describe the type of breach

- Location of Breached Information
- Select appropriate response (None, Laptop, Desktop Computer, Network Server, Email, or other portable electronic device) Network Server
- Was Substitute Notice Given?
    - Select appropriate response (N/A, No, Yes) No
- Was Media Notice Given?
    - Select appropriate response (N/A, No, Yes) No

Section II - Information for Law Enforcement Purposes

The information provided in Section II is for DOJ only.

- Name of Company contact whom the Attorney General may contact for further information
    - Estela M. Valdez – General Counsel's Office
- Telephone Number
    - 212-640-1847
- Email Address
    - Estela.m.valdez@aexp.com
- Was a law enforcement agency notified regarding the breach?
    - Select appropriate response (N/A, No, Yes) Yes
- If Yes, name of the law enforcement agency and contact name and number
    - Enter Agency: Local Law Enforcement
- Was a police report filed?
    - Select appropriate response (N/A, No, Yes) Yes
- If Yes, police report number
    - Enter number
- Submit form

Date:

Name
Address
City, State, Zip Code

Dear [Name],

American Express® Card Account ending in: XXXXX

American Express is strongly committed to the security of all our Cardmembers' information and wants to inform you that a merchant where you have used your American Express Card for payment detected unauthorized access to their website.

At this time, we believe the merchant's affected data files included your American Express Card account number, your name and the expiration date on your card. Importantly, your Social Security number is not impacted and our systems do not show any indication of unauthorized activity on your Card account related to this incident.

Beyond our standard fraud controls, American Express has placed additional fraud monitoring on your Card, and we will contact you if we detect any unusual activity. Also, following our long-standing practice, we do not hold our Cardmembers liable for fraudulent charges. In addition to the actions American Express is taking, there are precautionary steps that you can take to get more information:

- We encourage you to remain vigilant over the next 12 to 24 months and regularly review your statements. If you notice any suspicious activity on your American Express Card account or suspect identity theft, notify us immediately by calling **1-855-693-2213**.
- You can also sign up to receive free alerts of irregular account activity via cell phone, PDA, pager, or e-mail by visiting **www.americanexpress.com/alerts**.
- Identity Theft Assistance is a free benefit available to all American Express Cardmembers and includes access to representatives who are on call 24 hours a day, seven days a week, to offer tips on how to be protected against identity theft. For more information about Identity Theft Assistance, call **1-800-297-7672** or visit: **www.americanexpress.com/idtheftassistance**.

- Review your credit reports. To obtain an annual free copy of your credit reports, visit **www.annualcreditreport.com**.

- Once you receive your reports, review them carefully for inquiries from companies you did not contact, accounts you did not open, or debts on your accounts that you cannot explain. Verify the accuracy of your Social Security number, address(es), complete name and employer(s). Notify the credit bureaus if any information is incorrect.
- **Contact the major credit bureaus directly at:**

Equifax:	Experian:	TransUnion:
1-800-685-1111	1-888-397-3742	1-800-916-8800

www.equifax.com www.experian.com www.transunion.com

- Consider a fraud alert by contacting the fraud department of the three major credit bureaus to request that a "fraud alert" be placed on your file, and include a statement that creditors must get your permission before any new accounts are opened in your name.
- **Report fraud by contacting the major credit bureaus directly at:**

Equifax:	Experian:	TransUnion:
1-800-525-6285	1-888-397-3742	1-800-680-7289
www.equifax.com	www.experian.com	www.transunion.com

- **File a police report.** Get a copy of the report to submit to your creditors and others that may require proof of a crime.
- **Contact the Federal Trade Commission (FTC).** The FTC provides useful information to identity theft victims and maintains a database of identity theft cases for use by law enforcement agencies. File a report with the FTC by calling the FTC's Identity Theft Hotline: 1-877-IDTHEFT (438-4338); by mail, Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, N.W., Washington DC 20580; or online at **www.ftc.gov/bcp/edu/microsites/idtheft/**. Also request a copy of the publication, "Take Charge: Fighting Back Against Identity Theft."
- **Keep a record of your contacts.** Start a file with copies of your credit reports, the police report, any correspondence, and copies of disputed bills. It is also useful to keep a log of your conversations with creditors, law enforcement officials, and other relevant parties.

Your privacy is a priority for American Express and we hope you find this notification beneficial. To keep you better informed, you may receive multiple notification letters if more than one of your American Express Card accounts was impacted.

If you have questions, please call **1-855-693-2213** and an American Express customer care professional will be happy to assist you.

Sincerely,

Stefanie Wulwick
Privacy Officer, U.S. Banks
American Express Company